知识管理论坛 ISSN 2095-5472 CN11-6036/C
Knowledge Management Forum

E-mail: kmf@mail.las.ac.cn
http://www.kmf.ac.cn

【学术探索】

政府数据开放网站的个人隐私保护政策比较研究

◎ 张建彬[1] 黄秉青[1] 隽永龙[1] 张明江[1] 周志峰[2]

[1] 国网山东省电力公司电力科学研究院 济南 250000 [2] 温州大学图书馆 温州 325035

摘要：[目的 / 意义] 政府数据开放网站是数据开放的载体，政府数据开放网站的个人隐私政策直接关系到开放过程中个人隐私是否得到充分保护。[方法 / 过程] 为优化我国政府数据开放网站个人隐私保护策略，推进数据开放，从政策框架、个人隐私采集、共享使用、保护措施等方面对国内外政府数据开放网站个人隐私保护政策进行系统比较。[结果 / 结论] 提出应出台个人隐私保护综合性法律、强化政府公务员业务素质培训、加强政府数据开放过程中个人隐私利用监管、规范外部链接等措施来完善我国政府数据开放网站个人隐私保护策略。

关键词：政府数据开放网站 个人隐私保护 政策比较

分类号：G202

引用格式：张建彬 , 黄秉青 , 隽永龙 , 等 . 政府数据开放网站的个人隐私保护政策比较研究 [J/OL]. 知识管理论坛 , 2017, 2(5): 390-397[引用日期]. http://www.kmf.ac.cn/p/1/658/.

大数据时代的到来，对政府管理产生了巨大影响，催生了政府数据开放。伴随着政府数据开放实践的展开与推进，学界与实务界日益关注并重视政府数据开放相关理论与实践问题研究，日渐成为一门“显学”。政府数据开放最早产生于西方国家，美国、欧盟、加拿大、澳大利亚等国已开展得卓有成效。西方国家纷纷建立专门的数据开放网站作为数据开放的载体，及时开放涉及公共服务的数据，以改善公民服务，让公民知晓公共政策，增进民主对话中公共参与。我国国家数据开放步伐紧跟美国等西方国家，在总结政府信息公开实践经验的基础上，国家层面于 2015 年发布了《促进大数据发展行动纲要》，要求 2018 年年底前，建成国家政府数据统一开放平台；浙江省等一些省级政府、武汉市等一些副省级城市相继建成、投用政府数据开放平台，推进透明行政，让数据惠民，开创新型政府管理模式。但随着政府数据开放的深入推进，数据开放网站的个人隐私保护问题不断受到关注，由于政府所开放的数

基金项目：本文系 2015 年度教育部人文社会科学研究青年基金“群体智慧视野下政府开放数据开发利用管理研究”（项目编号：15YJCZH244）研究成果之一。

作者简介：张建彬（ORCID: 0000-0002-6851-7909），中级政工师，博士，E-mail：358560157@qq.com；黄秉青（ORCID: 0000-0002-2755-5239），中级政工师，硕士；隽永龙（ORCID: 0000-0003-0477-5340），中级政工师；张明江（ORCID: 0000-0002-7763-2765），中级政工师，硕士；周志峰（ORCID: 0000-0003-2312-7605），馆员，博士研究生。

收稿日期：2017-05-28 发表日期：2017-10-13 本文责任编辑：王传清

知识管理论坛，2017(5):390-397
DOI：10.13266/j.issn.2095-5472.2017.042

据涉及公民个人隐私，或者政府出于提供优质服务等目的会收集涉及公民隐私的信息。个人隐私是可以识别出信息主体的个人信息。在政府数据开放过程中，个人隐私泄露主要涉及源头泄露——信息采集、过程泄露——信息共享使用、结果泄露——信息安全保障 3 个方面。因此，本研究对中外政府数据开放网站隐私保护政策的比较主要从上述 3 个方面展开，旨在为我国优化完善政府数据开放网站个人隐私保护政策，推进数据开放实践提供有益的借鉴。

1 政府数据开放对个人隐私保护带来的挑战

政府数据开放网站有别于其他政府网站，主要体现在：政府数据开放网站强调政府的主动性、服务性，突出以用户为中心的建设理念，注重用户个性化服务体验，需向用户提出完整的数据集。政府建立数据开放网站，推进数据开放，给个人隐私保护带来了新的挑战，主要有以下 4 个方面：

1.1 政府数据再利用增加了泄露隐私的风险

政府在数据开放网站上发布的数据，通常可以免费获取，这为社会公众，特别是企业开发利用数据提供了便利条件。如浙江政务服务网中“信用信息”专题中公布了公民从业资格信息，如文化经纪人从业信息、医师资格证书信息、护士执业注册信息、医师执业注册信息等，已开放的数据包括获得资格人员的姓名和获得日期，一些企业可以利用上述数据研究开发查询系统。同时，在电话实名制背景下，为达到商业目的，在得知公民姓名的前提下，一些企业可通过通讯公司获取公民的详细信息，进而引发公民个人隐私泄露。

1.2 政府部门及其公务员泄露隐私的风险

政府数据开放网站中富含大量的公民个人隐私，主要包括：政府公共数据库中自带的公民个人隐私；政府通过 cookies 抓取的公民浏览政府数据开放网站的相关信息；公民为获取公共服务，在政府网站进行注册所提供的个人隐私。政府部门及其公务员是接触、管理公民个人隐私的主体，若出现政府管控不严格，或对隐私的界定标准理解不一致，以及公务员信息素养不足、职业伦理操守不良等情况，都会产生公民个人隐私泄露的风险。

1.3 大数据挖掘技术增加了个人隐私泄露的风险

随着大数据技术的广泛应用，数据挖掘技术可以将看似不相关的碎片化信息进行分析，建立相关关系，在不知不觉中侵犯公民隐私。大数据导致隐私信息市场的形成，这些市场的最初目的不是为了侵犯个人隐私，但结果却恰恰相反 [1]。大数据促进了数据内容的交叉检验，仅靠技术手段保护个人隐私将愈发困难。政府建立数据开放网站，发布一些公共服务信息，这些信息中本身就包含个人隐私，这为一些商业企业利用大数据挖掘技术获取有价值的个人隐私提供了可能。

1.4 信息安全问题易引发个人隐私泄露

随着信息通讯技术的高度发展，入侵技术等不断更新换代，攻击特定网站的能力日益增强。公民为获取公共服务或咨询政府问题，必然要提供一些个人隐私，因此，政府数据开放网站掌握着大量的个人隐私。虽然目前现有政府数据开放网站都声称将采取尽可能的技术措施有效防护网站安全，但仍存在一定风险，一旦网站被攻入，将给个人隐私带来不可挽回的损失，个人隐私可能会被大量窃取、侵犯。也正是由于这一担忧，一些政府部门才在数据开放方面表现迟钝、呈现观望态度。政府数据开放与个人隐私保护存在一定矛盾，这要求政府采取有力措施确保不发生信息安全危机事件。

2 政府数据开放网站个人隐私保护政策的比较分析

通过对国内外政府数据开放开展得比较好的国家和地方政府网站进行调研，研读各数据开放网站所发布的隐私政策，系统比较各级政府在数据开放过程中如何对个人隐私进行保护，以期为推进我国政府数据开放工作提供有

价值的建议。国外政府主要选取了数据开放实践开展得较早且较好的国家和组织，包括美国、欧盟、加拿大和澳大利亚；国内主要选取了已建成投用政府数据开放平台的一些省级政府和副省级城市，包括北京市、上海市、浙江省、广东省、贵州省和武汉市、广州市、深圳市、青岛市。

2.1 个人隐私保护政策总体情况比较

通过网站调研可以发现，国内外政府数据开放网站基本都设有隐私保护政策。我国一些地方政府数据开放平台的隐私政策嵌入在免责声明中，如青岛市政府、广州市政府。从公共政策角度来审视，政策本身的质量直接影响其所涉内容的落实及执行度。隐私政策内容的完整性、具体与否直接影响政府对公民个人隐私的保护力度及政策执行度。根据欧盟的观点，一个完整、详细的个人隐私保护政策或声明应包括：采集哪些信息、向谁公开信息、公民如何获取自己的信息、公民信息会被保存多久、采取的安全防护措施、问题咨询电话[2]。仔细研读各政府或组织的隐私政策内容发现，美国、欧盟、加拿大、澳大利亚和贵州省政府都对个人隐私的采集、处理、公开、使用及保护措施等环节进行了明确规定；上海市对采集与共享个人隐私的例外情况进行了说明；浙江省、广东省对共享个人隐私及保护措施进行了规范；北京市、武汉市、深圳市、广州市、青岛市只指出尊重并保护网站用户的个人隐私权，并表示未经用户许可或法律法规强制规定，不主动将个人信息泄露给第三方。另外，因西方国家大多出台了专门性个人隐私保护法律，故其政府数据开放网站上的个人隐私政策都有明确的法律遵循，而我国虽然出台了专门领域的个人信息保护法，如 2012 年出台的《关于加强网络信息保护的决定》，但缺乏一部个人隐私保护的综合性专门立法。因此，我国地方政府数据开放网站对个人隐私的保护没有明确的法律依据，仅指出遵循我国有关互联网管理相关法律法规。一些政府为提高公民的个人隐私保护意识，在隐私声明中加入了一些提醒或注意事项，如告知公民不要公开敏感信息或留意数据开放网站所外链的网站隐私保护政策等。另外，在个人隐私保护政策方面，国内外政府或组织数据开放网站的一个显著区别是，国内政府或组织在隐私保护政策或免责声明中都明确指出了因信息安全或信息再利用导致的隐私泄露，数据开放平台不承担任何责任，而国外政府数据开放网站无此规定。

2.2 政府数据开放网站个人隐私采集政策比较

从个人隐私泄露的链条来看，信息采集是源头。政府数据开放网站采集个人隐私的多少直接关系到个人隐私泄露带来的危害大小。美国、欧盟、加拿大和澳大利亚政府在数据开放网站中基本都给出了哪些个人隐私会被采集，或者要获取政府公共服务，公民需要提供哪些个人信息。在美国，当用户访问数据开放网站时，如果用户不主动提供，网站将不主动采集个人信息，但会采集 IP 地址、访问时间、搜索的文件名或关键词、网页中点击的项目、所使用的操作系统和浏览器[3]。网站为了技术目的使用 cookies 收集用户信息，但用户有拒绝 cookies 采集信息的自主权且不影响服务体验。当与政府对话或咨询问题时，用户可以选择性地提供电子邮件地址，无需提供额外个人信息，特别是社会保障号码。另外，美国还有一个特色信息采集模式，当用户以联邦、州、地方政府或司法机构代表身份以及非政府组织身份，为了获取行政特权以运用数据开放网站功能时，网站会收集名称、组织机构、职称、营业地、办公电话和办公邮件地址等信息。与其他政府或组织不同的是，美国专门将未成年人的隐私保护在隐私声明中予以单列。在欧盟，用户无需提供任何信息便可访问大部分网站，此外，政府为了提供公民所需的电子化公共服务，如信息服务、互动交流服务和交易服务，需要公民提供个人隐私。在加拿大，政府将 IP 地址作为个人信息予以保护，因为 IP 地址是一个独特号码，本身无法识别个人，但是

知识管理论坛，2017(5):390-397
DOI：10.13266/j.issn.2095-5472.2017.042

如果与其他数据相关联，如网站采集的访问时间等，便可识别出某个人在使用此网站。加拿大政府数据开放网站采集个人隐私秉持信息主体同意、认可的原则，在收集信息之前会征询信息主体同意，并告知其收集的目的及如何行使个人更正信息等权利，在某些情况下，制定有个人信息收集说明 [4]。如果通过电子邮件或提交完整反馈表形式与政府进行沟通，用户的个人信息将被收集。在澳大利亚，使用政府数据开放网站服务，用户无需提供可识别出个人的信息，但在与政府联系或需要政府反馈时，政府将会收集用户的电子邮件地址、姓名、电话号码等可以识别的个人信息。网站会使用 cookies 收集用户的偏好等信息，以开展网站分析、改善服务体验，用户有拒绝 cookies 采集信息的自主权，但与美国不同，一旦用户拒绝会影响服务体验。

我国各地方政府数据开放平台个人隐私采集政策参差不齐，既有详细说明如何收集及收集哪些信息的高质量政策，如贵州省政府，又有大而概之、笼统提及隐私保护的政策，如北京市、广东省、浙江省、武汉市、深圳市、广州市、青岛市。当用户访问数据开放平台时，贵州省所收集的用户信息范围与美国政府相同，政府数据开放网站采集用户的以下信息：IP 地址、访问时间、搜索的文件名或关键词、网页中点击的项目、所使用的操作系统和浏览器。与澳大利亚政府类似，贵州省政府数据开放网站会使用 cookies 收集用户的偏好等信息，以开展网站分析、改善服务体验，用户有停用 cookies 采集信息的自主权，但一旦用户停用会影响服务获取。另外，当用户进行注册登记、定制服务或参与网站调查时，需要提供很多个人隐私且信息必须是真实的，包括但不限于姓名、性别、身份证号码、电话、电子邮箱地址、职业、教育程度等 [5]。上海市无需注册即可浏览或下载数据开放网站上的所有内容，但如通过网站发布并提供数据应用服务或与政府部门进行交流，则需提供个人信息。

通过以上分析可发现，用户在政府数据开放网站获取个性化政府公共服务或与政府互动交流时，政府会收集公民的个人隐私，如姓名、电子邮箱地址等。政府收集这些信息的目的通常是了解用户的偏好与需求，以更好地、更精准地向用户提供满意的公共服务。但是，数据开放网站采集大量的公民个人隐私可能会带来隐私泄露的风险。

2.3 政府数据开放网站个人隐私共享使用政策比较

从目前我国实践来看，个人隐私泄露发生在共享使用环节居多，因此，政府在共享使用方面所采取的政策对个人隐私保护至关重要。在美国，为了科学研究目的，政府会向第三方机构分享、开放一些个人信息，如所采集的用户访问或浏览信息、IP 地址、访问时间等。此外，若公民所需公共服务涉及多个政府部门或依法律要求，政府会将一些个人信息与相关部门进行共享。在加拿大，通常政府不会将用户个人信息透露给任何人，除非政府雇员履行职能时需要这些信息。如果用户在网站上选择了需要其他政府部门或机构提供的项目或服务时，需要关注该机构的隐私注意事项，对于通过互动交流所采集的个人隐私，将被用于政府统计、评估以及制作报告。在欧盟，公民为获取电子化公共服务需要提供个人信息，政府部门隐私管控者对这些数据的处理方式和目的进行审查，以确保具体电子化服务符合隐私政策要求。在澳大利亚，除了防范非法活动或对健康、安全构成严重威胁，政府不与其他部门分享个人隐私；与美国、欧盟、加拿大不同，在向公民提供跨部门的政府服务时，除非公民本人同意或法律有规定，否则不与相关政府部门或机构分享公民信息，而是告知公民相关处理意见，如联系哪个相关部门获取政府服务 [6]。上海市对政府数据开放网站提供的数据再利用行为进行了规范，再利用者需要接受政府数据服务网用户协议约束，对于所采集的个人隐私，不会向任何第三方提供、出售、出租、分享和交

易，除非是基于为用户提供有效答复的需要[7]。贵州省明确列出了所采集个人隐私的用途，包括：①核实用户身份，并提供相应服务；②通过发送电子邮件或以其他方式，告知用户相关信息；③执行用户的指示、回应用户或以该用户名义提出的查询、建议或举报内容；④用于用户在提供信息时用于特定的目的，例如参与网上调查等。与澳大利亚相类似，贵州省给出了限制使用原则，在下列情况下，对所收集的个人隐私进行限制使用：已取得用户同意，为增进公共利益且无损于用户的重大利益等[5]。北京市[8]、武汉市[9]、深圳市[10]、广州市[11]和青岛市[12]5 个政府数据开放平台的个人隐私共享使用政策相同，都指出未经用户许可或根据相关法律法规的强制性规定，本网站不会主动将用户个人信息泄露给任意第三方。而浙江省[13]和广东省[14]的共享使用政策相同，都明确规定除用户同意和确认、国家法律法规规定、以及维护数据开放网站合法权益这 3 种情况外，不会将所采集个人隐私提供给第三方，并根据工作需要与政府有关部门共同使用个人隐私。这表明浙江省和广东省的共享使用政策保护力度明显弱于我国其他省政府。

通过上述分析可发现，虽然各国政府数据开放平台中个人隐私共享使用政策规定不尽相同，但存在一些共性。除美国为了科研目的公开信息外，各国政府数据开放网站基本采用积极的个人隐私共享使用政策，都不会主动公开或与第三方机构、个人共享个人隐私；各国政府或组织共享和利用个人隐私都基于公共性需要，包括满足公民个性化服务需求，为了公共利益或公民健康、安全免于威胁，行使公共职权需要等。虽然有学者宣称大数据时代告知与许可隐私保护策略已经失效[15]，但作为负有公共责任的政府，在处理公民个人隐私时需要有别于私营企业，需要尊重并保护公民个人隐私权，也正是基于此，多数政府或组织将信息主体的同意与许可作为个人隐私共享使用的一项基本原则。

2.4 政府数据开放网站个人隐私保护措施政策比较

政府对个人隐私的保护力度直接决定了个人隐私泄露风险大小及危害程度。保护措施是个人隐私安全与否的最后一道防线。政府数据开放平台是政府主办的安全、认证的设施，政府有责任、有义务做好安全防护。各政府数据开放网站都对个人隐私保护措施进行了规范，但详细程度不一，力度也有所区别。在美国，数据开放网站会提醒用户，开展网上评论时不要提供电子邮箱地址、电话号码等可以识别出个人的信息。同时，美国政府较为注重开展隐私影响评估，对采集可识别个人信息的系统进行评估，并审查个人隐私是否得到了充分保护。美国政府强化网络安全保护，采取物理、电子和程序性安全防护措施以保护个人隐私安全，并对非法攻击或上传、更改信息的行为进行严格限制，并依据计算机犯罪、滥用法和国家信息基础设施保护法进行惩罚。在加拿大，政府采取软件程序监测、识别上传和更改等引起危害的不法攻击，并将这些信息与执法部门进行分享，以优化网站安全策略，提高安全水平。在澳大利亚，政府采用物理、技术和行政措施来保护所采集的个人隐私，并不断更新和测试安全技术。为确保个人隐私安全，澳大利亚政府注重对雇员开展保密重要性培训，在政府公务员向公民提供公共服务时，即使需要使用公民个人隐私，这种使用行为也是受到严格限制的。根据欧盟出台的《关于个人数据处理及其自由流动的保护指令》（1995 年）和《关于个人数据处理及其自由流动的保护规定》（2012 年）相关规定，在每个政府部门专门设置了数据保护官员，以确保政府公共服务过程中严格执行个人数据保护法律法规规定，并向政府部门数据管控者提出建议。另外，欧盟还设有数据保护监督官，是独立于所有政府部门的监督机构，专司政府个人隐私保护情况监督。

我国各地方政府的个人隐私保护策略不尽相同。上海市充分利用现有技术保护数据开放

知识管理论坛，2017(5):390-397
DOI：10.13266/j.issn.2095-5472.2017.042

平台以及所有存储和传输的用户资料，并对因计算机病毒或其他非法软件导致的泄密事件依法追究责任[7]。贵州省、浙江省和广东省采用技术措施对数据开放平台所采集的个人隐私进行妥善保管，对因不可抗力或计算机病毒感染、黑客攻击等特殊原因造成的个人隐私泄露，数据开放平台将采取必要措施减少用户损失。而北京市、武汉市、深圳市和广州市只简单提及尊重并保护所有网站用户的个人隐私权，没有给出具体保护措施。青岛市的保护措施比较有特色，因多条数据关联后可能造成隐私泄露，网站有权随时将其下线，公众不得以任何理由继续保存或使用该数据；公众在使用网站提供的数据和服务时，应遵守有关法律、法规规定，不得用于任何可能侵犯个人隐私的用途[12]。另外，为了向公民提供优质公共服务，政府数据开放网站上提供了很多相关的外部链接，外部网站的隐私保护策略与数据开放网站不同，国内外政府基本都在隐私声明中提醒用户注意查看外部链接网站的隐私政策。

通过上述分析发现，与国外政府采取多种措施保护个人隐私不同，我国各地方政府数据开放平台个人隐私保护手段较为单一，主要采取技术手段开展保护，而且，针对非法入侵网站等导致个人隐私泄露的事件，各政府没有充分利用法律武器追究责任。

3 借鉴与启示

国外政府在推进政府数据开放实践中，采取了诸多个人隐私保护举措，很多卓有成效的做法值得我国学习与借鉴。为进一步做好政府数据开放中个人隐私保护，推进数据开放，我国需要在现有的技术保护以外采取下列措施：

3.1 制定个人隐私保护综合性法律，做到有据可依

美欧等国家或组织政府数据开放过程中的个人隐私保护，都有明确的个人隐私保护法作为准绳，个人隐私综合性法律明确规定了个人隐私保护的范围，如欧盟个人数据保护法指出，身份证号码、定位数据、网络标识符、生理、心理、基因、精神、经济、文化、社会身份等隐私受法律保护[16]。个人隐私保护法可以明确地规定隐私保护范围，以及规范政府等组织采集、共享使用个人隐私行为，并要求隐私采集、使用者采取相应防护措施。在立法过程中需要注重质量，保护范围上应采取列举方式详细说明，以下信息必须纳入保护范围：①与公民个人的住址、身份证号、照片、联系方式、教育背景、工作履历、婚姻状况的相关信息；②与公民的健康信息及疾病史、指纹相关的信息；③与公民个人的政治观点或看法、交易记录、犯罪前科相关的信息；④与公民个人的信函、电子邮件、日记相关的信息；⑤与公民个人的驾驶执照号、交通记录、通信记录相关的信息。当然，保护公民个人隐私的法律法规中，需要对采集和使用个人隐私的目的合法性、合理性等原则做出规定，并对例外情况进行规定，如为了信息主体的健康和公共利益、安全等，可在未经信息主体同意的情况下直接使用个人隐私信息，与个人的犯罪事实相关的信息不在法律保护范围内。此外，法律法规中应对个人隐私泄露造成的危害进行细化、量化，以便司法机关进行司法实践，并将利用他人隐私对他人生活进行骚扰而未造成实质损害的行为纳入法律惩处。国家出台综合性个人保护法律可以使政府数据开放网站的隐私保护政策有明确的依据，隐私政策的内容和质量亦将进一步丰富、完善。

3.2 强化政府公务员业务素质培训

政府公务员所从事的是一种特殊职业，他们应是“职业公民”和负责任的行政人员[17]。社会公众对政府公务员具有角色期待，这种期待要求公务员具有良好的职业操守和行政伦理，开展责任行政。良好的职业操守和行政伦理的形成，除了内在的自我约束外，关键在于外在培养，通过开展广泛培训提升公务员的内在品质。例如：①组织政府公务员到美国等发达国家进行实地考察，深入学习政府数据开放中个人隐私保护的具体做法，以增强保密重要性与保护

个人隐私的认知；②对政府公务员进行相关培训，邀请个人隐私保护研究领域的国内外专家学者进行授课，使政府公务员知晓如何保护个人隐私，以及泄露个人隐私将受到的惩罚等。通过提高政府公务员的职业操守，使政府公务员在数据开放过程中自觉保护所接触的个人隐私，有效避免因工作疏忽或失误导致的个人隐私泄露。

3.3 加强政府数据开放过程中个人隐私监管

为消除一些政府部门及其工作人员出售、泄露、不合理使用个人隐私信息的现状，建议将持有个人隐私的政府部门及其工作人员是否合法、合理采集和使用个人隐私纳入单位领导及工作人员的绩效考核，将其作为一项重要考核指标，并将考核结果与相关人员的奖惩相结合；而对于违法采集、泄露、出售、使用个人隐私的政府部门及其工作人员，则要进行通报批评；对信息主体造成损害的，无论是物质、精神、人身安全上的损害，都要依法追究相关责任人的民事和刑事责任。另外，结合我国政府信息公开实践中的机构设置，建议在政府信息公开办公室中设置信息保护官，专司监督数据开放过程中个人隐私是否严格依法得到了充分保护，并对各政府部门采集、使用个人隐私进行全过程审查。

3.4 规范政府数据开放网站的外部链接

政府数据开放网站是由政府建立、为公民提供便利电子化服务的载体。政府为了向公民提供完整、优质的公共服务，会允许一些社会化网站链接到政府数据开放平台，以便于公众快速获取所需的服务。政府作为负有公共责任的组织，是数据开放过程中个人隐私保护的主体，有责任、有义务制定外部链接的许可标准，并开展外部链接审查，对隐私保护策略不合格的网站禁止外联，以有效避免因政府数据开放网站外部链接所引起的个人隐私泄露。

参考文献：

[1] COHEN J E. Privacy, visibility, transparency, and exposure[J]. The University of Chicago law review, 2008, 75(1): 181-201.

[2] Information contained in a specific privacy statement[EB/OL]. [2017-03-09]. https://ec.europa.eu/info/legal-notice_en#disclaimer.

[3] Privacy policy[EB/OL]. [2017-04-10]. https://www.data.gov/privacy-policy.

[4] Privacy[EB/OL]. [2017-04-10]. https://www.canada.ca/en/transparency/privacy.html?_ga=1.254538688.975917455.1483360555.

[5] 贵州省政府数据开放平台隐私声明 [EB/OL]. [2017-05-10]. http://www.gzdata.gov.cn/privacy.html.

[6] Privacy policy[EB/OL]. [2017-05-10]. http://data.gov.au/about.

[7] 上海市政府数据服务网使用条款 [EB/OL]. [2017-05-10]. http://www.datashanghai.gov.cn/home!toUseProvisions.action.

[8] 北京市政务数据资源网隐私保护声明 [EB/OL]. [2017-05-11]. http://www.bjdata.gov.cn/gywm/mzsm/index.htm.

[9] 武汉市政府公开数据服务网隐私保护声明 [EB/OL]. [2017-05-20]. http://www.wuhandata.gov.cn/whdata/disclaimer.jsp.

[10] 深圳市政府数据开放平台隐私保护声明 [EB/OL]. [2017-05-20]. http://opendata.sz.gov.cn/common/toserviceTerms.

[11] 广州市政府数据统一开放平台隐私保护声明 [EB/OL]. [2017-05-22]. http://datagz.gov.cn/data/sitelaw.htm.

[12] 青岛市政府数据开放网站免责声明 [EB/OL]. [2017-05-24]. http://data.qingdao.gov.cn/data/interact/law.htm.

[13] 浙江政务服务网隐私保护 [EB/OL]. [2017-05-25]. http://www.zjzwfw.gov.cn/col/col42277/index.html.

[14] 广东省开放数据管理平台隐私保护声明 [EB/OL]. [2017-05-28]. http://www.gddata.gov.cn/index.php/Index/ArticleDetails/id/5.html.

[15] 迈尔 - 舍恩伯格 , 库克耶 . 大数据时代 : 生活、工作与思维的大变革 [M]. 盛杨燕 , 周涛 , 译 . 杭州 : 浙江人民出版社 , 2013: 200.

[16] European Commission. Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation) [EB/OL]. [2017-06-10]. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[17] 丁煌 . 西方行政学理论概要 [M]. 北京 : 中国人民大学出版社 , 2003: 308-327.

作者贡献说明：

张建彬：负责文章执笔，并审核文章内容；
黄秉青：参与国外政府数据公开网站的信息收集及翻译工作；
隽永龙：负责省级政府数据公开网站相关信息收集加工；
张明江：负责副省级城市政府数据公开网站相关信息收集加工；
周志峰：负责文章的校对，并对文章内容提出了一些修改建议。

知识管理论坛，2017(5):390−397
DOI：10.13266/j.issn.2095−5472.2017.042

Comparative Study on the Personal Privacy Protection Policies of Open Government Data Websites

Zhang Jianbin[1] Huang Bingqing[1] Jun Yonglong[1] Zhang Mingjiang[1] Zhou Zhifeng[2]
[1]State Grid Shandong Electric Power Research Institute, Jinan 250000
[2]Wenzhou University Library, Wenzhou 325035

Abstract: [Purpose/significance] The open government data website is the carrier of the open data, and the personal privacy protection policy of the open government data website is directly related to personal privacy protection in the process of opening government data. **[Method/process]** In order to optimize the personal privacy protection policy of open government data websites and promote open data, this paper compared personal privacy protection policies of domestic and foreign government open data websites in terms of the policy framework, personal privacy collection, sharing and protection measures. **[Result/conclusion]** It points out that governments should formulate comprehensive laws on personal privacy protection, strengthen the government official quality training, reinforce the privacy usage supervision in the process of open government data and standardize external links and other measures to improve personal privacy protection policies of open government data websites.

Keywords: open government data website personal privacy protection policy comparison